	DESCRIÇÃO	
01	Solução de gerência de rede sem fio (WLAN)	01
02	Ponto de acesso sem fio (Access Point-AP)	320
03	Switch de acesso PoE	35
04	Controladora Wireless	02
05	Pacote de Licenças para usuários visitantes (500 usuários)	02
06	Solução de Controle de Acesso	01
07	Serviços de instalação e configuração dos itens 1,4,5 e 6	01
08	Serviços de instalação e configuração dos pontos de acesso e switches PoE (itens 2 e 3)	320
09	Treinamento	02
10	Site Survey	06

ANEXO I – Descrição dos Itens e Serviços

1. **Solução de Gerência de Rede Sem Fio (WLAN)**

1.1. Deverá ser totalmente compatível com o ponto de acesso e a controladora *wireless* solicitados neste processo, sendo que as funcionalidades descritas a seguir são complementares à controladora de rede sem fio e podem ser atendidas por qualquer um dos componentes da solução, ou seja, a funcionalidade pode estar presente na controladora de rede sem fio ou no software de gerência;

1.2. Deverá gerenciar todos os pontos de acesso e controladores *wireless*, especificados nesta solução de rede sem fio (WLAN), de maneira centralizada.

1.3. A solução deverá suportar arquitetura distribuída e mecanismo de alta disponibilidade;

1.4. Permitir instalação em ambiente virtual *VMware ESXi* 6.0 ou superior;

1.5. Suporte aos sistemas operacionais RedHat Enterprise Linux ou CentOS 7 ou Windows Server 2012 ou superior, em plataforma de hardware padrão Intel;

1.6. Deverá ser fornecida pela CONTRATADA as licenças do sistema operacional e do banco de dados, caso haja a necessidade desses recursos;

1.7. As licenças deverão ser de caráter permanente, por tempo indeterminado, permitindo que todas as funcionalidades e características da solução de rede sem fio estejam operantes mesmo após a vigência do contrato ou garantia da solução;

1.8. O *software* deverá permitir expansão gradual ou modular dos recursos de gerenciamento, mediante adição de novas licenças, tanto para gerência de até 500 (quinhentos) de pontos de acessos quanto para incremento de usuários/clientes, visitantes e dispositivos;

1.9. Deve ser possível fazer a gerência de configuração dos pontos de acessos incluindo backup, upgrade de *software* e arquivos de configuração por meio de *software;*

1.10. Deve ser fornecida uma licença vitalícia do *software* de gerência do fabricante da respectiva controladora;

1.11. Permitir a atualização remota do sistema operacional e dos arquivos de configuração utilizados no ponto de acesso e registro de sucesso e eventuais problemas durante o processo;

1.12. Permitir notificações e envio por e-mail quando um relatório for gerado manualmente, com opção de customização;

1.13. Coletar eventos da rede sem fio (WLAN) e disponibilizar, em interface gráfica, informações em tempo real;

1.14. Possibilitar a visualização, em interface gráfica ou relatório customizado, das seguintes informações sobre a rede sem fio:

1.14.1. Listagem de pontos de acesso;

1.14.2. Listagem de clientes wireless por utilização ou tipo de dispositivo;

1.14.3. Utilização de dados (consumo de banda) por ponto de acesso;

1.14.4. Disponibilidade dos pontos de acesso (uptime);

1.14.5. Informações sobre pontos de acesso não autorizados (rogues) intrusos na rede (wireless intrusion);

1.15. Deve possuir funcionalidade baseada em reconhecimento de aplicações que permita ao administrador da rede identificar quais aplicações estão sendo trafegadas na rede wireless por dispositivo ou por usuário/perfil.

1.16. Deve possuir mecanismos para consolidar informações de rede, tais como: relação sinal/ruído, interferência, potência de sinal, etc., permitindo ao administrador isolar e resolver problemas nos vários níveis da rede;

1.17. Possibilitar a visualização, em interface gráfica ou relatório customizado, das seguintes informações sobre os clientes conectados à rede sem fio:

1.17.1. Endereço IP;

1.17.2. Endereço MAC;

1.17.3. SSID;

1.17.4. Canais utilizados;

1.17.5. Ponto de acesso ao qual está associado;

1.17.6. Dados de associação e autenticação;

1.17.7. Dados sobre as aplicações trafegadas;

1.18. Permitir a visualização e armazenamento das informações históricas, internamente à solução, por um período mínimo de 14 (quatorze) dias, sobre autenticação de usuários da rede sem fio, tanto da rede coorporativa (802.1x) como da rede guest (captive portal);

1.19. Implementar servidor de syslog ou permitir o redirecionamento de eventos para servidor de syslog;

1.20. Permitir a configuração e gerenciamento por meio de browser padrão, com suporte ao protocolo HTTPS;

1.21. Deverá possibilitar a importação de plantas baixas nos formatos dwg ou jpg ou png, devendo permitir a visualização dos pontos de acesso instalados, com seu estado de funcionamento.

1.22. Possuir modelos de configuração (templates) de forma a possibilitar a replicação de configuração entre equipamentos.

1.23. Permitir a criação de hierarquia de administradores das redes sem fio (WLAN), criando visões administrativas independentes.

2. **Ponto de Acesso Sem Fio (Acess Point-AP)**

2.1. Possuir certificado de homologação emitido pela Anatel.

2.2. Possuir certificado emitido pelo “WIFI Alliance” na categoria de Enterprise Access Point;

2.3. Permitir a atualização remota do sistema operacional, firmware e dos arquivos de configuração utilizados no equipamento;

2.4. Permitir a configuração e gerenciamento através do Browser padrão HTTPS, SSH, ou porta de console para gerenciamento e seu respectivo cabo para as configurações via linha de comando CLI

2.5. Possuir LED para indicar o status, falhas ou alarmes do ponto de acesso, dos rádios e das portas de rede;

2.6. Possuir cliente DHCP, para configuração automática do seu endereço IP assim como endereçamento IP estático;

2.7. Suportar configuração para permitir conexão simultânea de dispositivos em 2.4GHz e 5GHz;

2.8. Implantar ajuste dinâmico de nível de potência e canal de rádio;

2.9. O Equipamento de ponto de acesso sem fio deverá atender aos padrões IEEE 802.11a, IEEE 802.11b, IEEE 802.11g, IEEE 802.11n e IEEE 802.11ac (compatível com padrão wave 2), com configuração via software.

2.10. O equipamento deve ser gerenciável pelo software de gerência ou controladora de rede sem fio (WLAN) especificado no item 01 e 04 para configuração de seus parâmetros *wireless*, gerenciamento das políticas de segurança, QoS e monitoramento de rádio frequência (RF);

2.11. Possuir licenças necessárias para o gerenciamento via software de gerência ou controladora rede sem fio (WLAN) conforme descrito no item 1 e 4.

2.12. O ponto de acesso deverá associar-se automaticamente à outra controladora wireless alternativa em caso de falha da controladora atualmente conectada, sem permitir que a rede sem fio se torne inoperante;

2.13. Armazenar sua configuração em memória não volátil, podendo, em uma queda e posterior restabelecimento da alimentação, voltar à operação normalmente na mesma configuração anterior;

2.14. Permitir simultaneamente usuários configurados nos padrões IEEE 802.11b/g/n (2.4 GHz) e 802.11a/n/ac (5 GHz), através de rádios independentes (*dual radio*);

2.15. Possuir antenas compatíveis com as frequências de rádio dos padrões IEEE 802.11a/b/g/n/ac (wave 2) com padrão de irradiação omnidirecional.

2.16. Possuir potência de transmissão total (EIRP) de, no mínimo, 22dBm em 2.4GHz e 5GHz.

2.17. Deve operar com sensibilidade mínima de -91 dBm

2.18. Deverá possuir mecanismo de rádio com suporte à 2X2 MU-MIMO (Wave2), com 2 Spatial Streams ou superior, para o rádio de 2,4GHz.

2.19. Deverá possuir mecanismo de rádio com suporte à 3X3 MU-MIMO (Wave2), com 3 Spatial Streams ou superior, para o rádio de 5GHz.

2.20. Possuir as seguintes taxas de transmissão e com fallback automático:

2.20.1. IEEE 802.11a: 54, 48, 36, 24, 18, 12, 9 e 6 Mbps;

2.20.2. IEEE 802.11b: 11 e 1 Mbps;

2.20.3. IEEE 802.11g: 54, 48, 36, 24, 18, 12, 9 e 6 Mbps;

2.20.4. IEEE 802.11n: 6.5 a 300 Mbps (MCS0 a MCS15), 1 a 2 Spatial Streams;

2.20.5. IEEE 802.11ac: 6.5 a 1,300 Mbps (MCS0 a MCS9), 1 a 3 Spatial Streams;

2.21. Deverá suportar VLAN seguindo o padrão IEEE 802.1.q;

2.22. Permitir que a comunicação com o software e controladora rede sem fio (WLAN) especificado no item 01 e 04 seja criptografada;

2.23. Possuir o protocolo de enlace CSMA/CA (Carrier Sense Access/Colission Avoidance) e operar nas modulações DSSS, OFDM e 802.11n e 802.11ac Wave 2;

2.24. Suportar os seguintes métodos de modulação:

2.24.1. 802.11b: BPSK, QPSK, CCK

2.24.2. 802.11a/g/n/ac: BPSK, QPSK, 16-QAM, 64-QAM, 256-QAM

2.25. Permitir, no mínimo, 200 (duzentos) conexões de dispositivos simultâneas, sem nenhum tipo de licença adicional;

2.26. Possuir capacidade de selecionar automaticamente o canal de transmissão;

2.27. Permitir a configuração de largura de canal de 20MHz (vinte mega-hertz) ou 40 MHz (quarenta mega-hertz) ou 80MHz (oitenta mega-hertz);

2.28. Permitir habilitar e desabilitar a divulgação do SSID;

2.29. Possuir padrão WMM da Wi-Fi Alliance para priorização de tráfego, suportando aplicações em tempo real, tais como VoIP e vídeo;

2.30. Possuir a pilha de protocolos TCP/IP;

2.31. Suportar a divulgação e utilização de, no mínimo, 8 (oito) BSSIDs por rádio;

2.32. Possuir diferentes tipos de combinações de encriptação e autenticação por SSID;

2.33. Suportar a autenticação com geração dinâmica de chaves criptográficas por sessão ou por usuário;

2.34. Possuir, no mínimo, 1 (uma) interfaces 10/100/1000BaseT Ethernet, auto-sensing, auto MDI/MDX, com conector RJ-45, para conexão com a rede local- LAN;

2.35. Suportar fonte de alimentação DC direta externa para alimentação elétrica.

2.36. Possuir Power over Ethernet (padrão IEEE 802.3af ou 802.3at), para alimentação elétrica. A alimentação elétrica deve ocorrer através de uma única interface de rede, sem perda de funcionalidade e de desempenho;

2.37. Possuir, em conjunto com o software de gerência ou controladora rede sem fio (WLAN) especificado no item 01 e 04, padrões abertos de gerência de rede SNMPv2c e SNMPv3, incluindo a geração de traps ou RestFull APIs;

2.38. Possuir em conjunto com o software de gerência ou controladora rede sem fio (WLAN) especificado no item 01 e 04, suporte a MIB (Management Information Base);

2.39. Possibilitar, em conjunto com software de gerência e controladora rede sem fio (WLAN) especificado no item 01 e 04, a obtenção via SNMP de informações de capacidade e desempenho;

2.40. Suportar os protocolos IPv4 e Ipv6;

2.41. Permitir roaming transparente sem troca de endereçamento IPV4 e IPv6 para clientes móveis;

2.42. Possuir, em conjunto com o software de gerencia ou controladora rede sem fio (WLAN) especificado no item 01 e 04, varredura de rádio frequência (RF) nas bandas 802.11a, 802.11b/g, 802.11n e 802.11ac (compatível com padrão wave 2) para identificação de pontos de acesso intrusos não autorizados (rogues access points) e interferências no canal habilitado ao ponto de acesso e nos demais canais configurados na rede sem fio (WLAN);

2.43. Possuir, em conjunto com o software de gerência ou controladora rede sem fio (WLAN) especificado no item 01 e 04, filtros de acesso à rede baseados em endereços MAC;

2.44. Possuir, em conjunto com o software de gerência ou controladora rede sem fio (WLAN) especificado no item 01 e 04, IEEE 802.1x, com pelo menos os seguintes métodos EAP: EAP-TLS e PEAP-MSCHAPv2;

2.45. Permitir, em conjunto com o software de gerência ou controladora rede sem fio (WLAN) especificado no item 01 e 04, a integração com Radius Server ou Microsoft Active Diretory para autenticação de usuários;

2.46. Possuir, em conjunto com o software de gerência ou controladora rede sem fio (WLAN) especificado no item 01 e 04, comutação do tráfego local, de maneira que o tráfego de determinado SSID possa ser comutado na rede local sem intervenção da controladora, exceto no aspecto de autenticação dos usuários;

2.47. Possuir, em conjunto com o software de gerência ou controladora rede sem fio (WLAN) especificado no item 01 e 04, WPA2 com algoritmo de criptografia AES, 128 bits, conforme padrão IEEE 802.11i;

2.48. Possuir a tecnologia de “Band Steering/Select”, permitindo que clientes se conectem aos pontos de acesso utilizando, preferencialmente, a faixa de 5GHz;

2.49. Possuir a tecnologia de “Beamforming” ou similar para melhorar o desempenho de transmissão de dados para determinados usuários da rede sem fio e aumentar o seu alcance;

2.50. Possuir, em conjunto com o software de gerência e controladora rede sem fio (WLAN) especificado no item 01 e 04, interface com informações gráficas de análise de espectro;

2.51. Deverá suportar o modo de operação de monitoramento que permite a prevenção de ataques e acessos não autorizados (WIPS), cobrindo todos os canais da faixa de frequências em que o rádio do ponto de acesso estiver operando (2.4GHz e 5GHz);

2.52. Ser capaz de operar, ao atendimento de clientes da rede sem fio, como sensor para análise de ameaças;

2.53. Possuir capacidade de identificação e listagem dos rádios vizinhos e respectivos SSID/BSSID;

2.54. Possuir antenas integradas e internas;

2.55. Possuir estrutura que permita fixação do equipamento em teto ou parede e fornecer todos acessórios para que possa ser feita a fixação;

2.56. Possuir trava padrão “Kensington security lock point” ou similar, acompanhado do Kit de segurança;

2.57. O ponto de acesso deverá vir com a versão mais recente de firmware, possibilitando integração total com a solução de rede sem fio e operação de todas as funcionalidades solicitadas nesta especificação técnica;

3. **Switch de acesso PoE**

3.1. Switch tipo acesso;

3.2. Deverá ter a arquitetura para ser montado em rack padrão de 19', com 1U de tamanho;

3.3. Deverá possuir fonte de alimentação interna o suficiente para alimentar os pontos de acesso com todas as suas funcionalidades habilitadas especificadas nesse projeto, com seleção automática de tensão 100/240V, e frequência de 50/60Hz;

3.4. Deverá ter no mínimo os seguintes tipos e velocidade de interface:

3.4.1. 24 portas 10/100/1000BaseT PoE+;

3.4.2. Suportar, pelo menos, 2 (duas) portas padrões 1000BASE-SX SFP, sendo que portas de console ou de gerenciamento não serão computadas para atender essa exigência;

3.4.3. Cada switch deverá vir acompanhada de 2 (dois) transceiver óptico padrão 1000Base-SX SFP, plenamente compatível com suas portas SFP;

3.4.4. Deve ser capaz de alimentar as 24 portas com o padrão PoE (IEEE 802.3af) e um mínimo de 12 portas com PoE+ (IEEE 802.3at).

3.5. Deverá ser fornecido 1 (um) cordão óptico duplex compatível para cada interface do item 3.4.2, para conexão das interfaces no DIO, considerando o seguinte:

3.5.1. O padrão de interface do Distribuidor é LC;

3.5.2. O cordão óptico deverá ter no mínimo 5m.

3.6. Deverá possuir o Switching capacity mínima de 52Gbps

3.7. Deverá possuir o Switching throughput mínimo de 38mpps em pacotes de 64bytes, expansível a configuração máxima de portas do chassi;

3.8. Deverá possuir no mínimo os seguintes recursos:

3.8.1. Layer 2 switching, Vlan - IEEE 8021q, Spanning Tree 802.1d/802.1.w/802.1s, Link Aggregation-802.3ad e Jumbo-Frames;

3.8.2. Gerenciamento SNMP V1/V2/V3, SSH, telnet, CLI e interface console;

3.8.3. Monitoramento de tráfego segundo RFC3176 ou recurso semelhante, mirroring port, RMON estatísticas;

3.8.4. Suportar pelo menos 16K endereços MAC;

3.8.5. Quality of Service (QOS), classificação de pacotes, priorização de tráfego (802.1p), marcação campo TOS, ACL e Vlan dinâmica por porta;

3.8.6. Proteção para ataques do tipo ARP, MAC, Broadcast Storm e DHCP;

3.8.7. Empilhamento para gerenciamento através de IP único.

3.9. O equipamento deve ser gerenciável pelo software de gerência ou controladora de rede sem fio (WLAN) especificado no item 01 e 04 com suas respectivas licenças, caso necessário;

3.10. Possuir FTP (File Transfer Protocol) ou TFTP (Trivial File Transfer Protocol) ou SFTP (Secure File Transfer Protocol) ou SCP (Secure Copy Protocol);

3.11. Deverá ser acompanhado de documentação técnicas e manuais que contenham informações suficientes para possibilitar a instalação, configuração e operacionalização do equipamento;

3.12. Deverá ser fornecido com todos os acessórios necessários para operacionalização do equipamento, tais como software, cabos lógicos, cabos de interface RS-232 ou USB ou RJ-45, cabos de energia elétrica e kit de fixação no rack.

4. **Controladora Wireless**

4.1. A solução para controladora poderá ser do tipo *appliance* virtual, totalmente compatível com a solução *VMware ESXi 6.0 ou superior*, já utilizada na estrutura de Datacenter da CONTRATANTE ou uma solução do tipo appliance físico;

4.2. Características comuns às tecnologias appliance virtual e física:

4.3. Deverá ser do mesmo fabricante dos pontos de acesso fornecidos pela CONTRATADA, para fins de compatibilidade e gerenciamento;

4.4. Deverá possibilitar a implementação de alta disponibilidade com a capacidade de redundância da controladora wireless, no modo ativo/ativo ou ativo/passivo, com sincronismo automático das configurações entre controladoras;

4.5. Deverá possuir capacidade de implementação de perfis de configuração de equipamentos, para a implementação de novos pontos de acesso sem a necessidade de configuração individual de cada equipamento (implementação zero-touch);

4.6. Deverá centralizar a manutenção e distribuição das configurações dos pontos de acessos;

4.7. Deverá controlar a configuração dos pontos de acesso gerenciados e otimizar o desempenho e a cobertura da radiofrequência;

4.8. Deverá permitir que os SSIDs operem em modo de tunelamento de tráfego remoto ou comutação de tráfego local;

4.9. Deverá permitir que os SSIDs possuam parâmetros de VLAN e QoS individuais;

4.10. Deverá prover priorização de tráfego de vídeo e voz através de parâmetros de QoS (Quality of Service) com possibilidade de aplicar por SSID ou dispositivo;

4.11. Deverá ter a capacidade para gerenciar, no mínimo, 320 (trezentos e vinte) pontos de acesso, podendo chegar através de atualização de licenças de software até 500 (quinhentos) pontos de acesso, simultâneos;

4.12. Deverá possuir capacidade para conexão simultânea de, no mínimo, 8.000 (oito mil) dispositivos wireless;

4.13. Deverá permitir que os usuários corporativos deverão se autenticar utilizando integração com LDAP e a autenticação de usuário visitante deverá ser feita através de integração com portal web (captive portal);

4.14. Deverá permitir a criação de múltiplos usuários visitantes (guests).

4.15. Deverá possuir autenticação via portal web (captive portal) para os usuários da rede wireless que não puderem se autenticar via 802.1x.

4.15.1. Esta solução de autenticação de usuários visitantes deve se integrar, mas não pode se confundir, com o licenciamento da controladora para os pontos de acesso;

4.16. Deverá possuir, em conjunto com o software de gerência, associação dinâmica de usuário a VLAN, com base nos parâmetros de autenticação;

4.17. Deverá permitir a utilização de portal web (captive portal) externo a controladora;

4.18. Deverá permitir o direcionamento do tráfego de saída de usuários visitantes (guests) para uma rede isolada do tráfego da rede corporativa;

4.19. Deverá conectar-se diretamente e/ou remotamente aos pontos de acesso, permitindo o gerenciamento de equipamentos em múltiplos sites;

4.20. Deverá possuir varredura de rádio frequência (RF) contínua, programada ou sob demanda, com identificação de pontos de acesso ou clientes irregulares;

4.21. Deverá ajustar automaticamente a potência dos pontos de acesso adjacentes, na ocorrência de inoperância de um ponto de acesso, de modo a minimizar a falta de cobertura em área não assistida;

4.22. Deverá ajustar automaticamente os canais de modo a otimizar a cobertura de rede e mudar as condições de rádio frequência (RF) baseado em performance;

4.23. Deverá detectar interferência e ajustar parâmetros de rádio frequência (RF), evitando problemas de cobertura e controle da propagação indesejada de rádio frequência (RF);

4.24. Deverá possuir varredura de rádio frequência (RF) nas bandas 802.11a, 802.11b, 802.11g, 802.1n e 802.11ac (compatível com padrão wave 2) para identificação de ataques e APs intrusos não autorizados (rogues);

4.25. Deverá identificar os pontos de acesso válidos, os pontos de acesso que interferem e os pontos de acesso que não são autorizados (rogues);

4.26. Deverá possuir mecanismo para notificar os pontos de acesso não autorizados (rogues) detectados;

4.27. Deverá permitir a criação de filtros e permitir a criação de regras para bloqueio das aplicações.

4.28. Deverá ajustar dinamicamente o nível de potência e canal de rádio dos pontos de acesso, de modo a otimizar o tamanho da célula de rádio frequência (RF), garantindo a performance e escalabilidade;

4.29. Deverá possuir padrão IEEE 802.11h que otimizam a transmissão via rádio e que o rádio ajuste a potência do sinal de acordo com a distância do receptor;

4.30. Deverá possuir a tecnologia de “load balancing”, permitindo que clientes sejam automaticamente distribuídos entre pontos de acesso adjacentes operando em canais distintos, com o objetivo de balancear a carga entre os pontos de acesso;

4.31. Deverá possuir, em conjunto com o ponto de acesso, QoS com suporte a WMM;

4.32. Deverá possuir padrão IEEE 802.1q (VLANs);

4.33. Deverá permitir a criação de pelo menos 256 (duzentos e cinquenta e seis) VLANs simultâneas;

4.34. Deverá suportar a criação, divulgação e utilização de, no mínimo, 128 (cento e vinte e oito) SSIDs simultâneos;

4.35. Deverá possuir padrão IEEE 802.1p (Priorização na camada MAC);

4.36. Deverá ter suporte aos protocolos IPv4 e IPv6;

4.37. Deverá possuir os protocolos NTP ou SNTP;

4.38. Deverá permitir a configuração e gerenciamento por meio de browser padrão, com suporte ao protocolo HTTPS; via linha de comando CLI e permitir gerenciamento seguro via SSHv2;

4.39. Deverá possibilitar a configuração completa de todos os componentes da rede sem fio (WLAN) em interface gráfica;

4.40. Possuir Fast BSS Transition de acordo com o padrão IEEE 802.11r para aceleração do roaming dos usuários;

4.41. Possuir o padrão IEEE 802.11k para permitir que um dispositivo conectado à rede wireless identifique rapidamente pontos de acesso próximos disponíveis para roaming;

4.42. Permitir a gravação de eventos por meio do protocolo syslog com possibilidade de redirecionamento para ferramentas de terceiros;

4.43. Possuir padrões abertos de gerência de rede SNMPv2c e SNMPv3, incluindo a geração de traps ou RestFull API;

4.44. Os padrões SNMP deverá:

4.44.1. Possuir suporte a MIB II, conforme RFC 1213.

4.44.2. Possuir a MIB privativa que forneça informações relativas ao funcionamento do equipamento;

4.44.3. Possuir descrição completa da MIB implementada no equipamento, inclusive a extensão privativa;

4.45. Possuir IEEE 802.1x, para autenticação de clientes wireless, com pelo menos os seguintes métodos EAP: EAP-TLS e PEAP-MSCHAPv2;

4.46. Permitir a utilização de Radius Server ou Microsoft Active Directory que suporte os métodos EAP citados no subitem anterior;

4.47. Deverá permitir a configuração e operação de no mínimo dois servidores RADIUS para fornecer redundância na autenticação;

4.48. Na ocorrência de falha na comunicação com o servidor RADIUS principal, o sistema deverá buscar um servidor RADIUS secundário.

4.49. Deverá permitir a seleção/uso de servidor RADIUS com atributos “radius standard”;

4.50. Deverá permitir a limitação de banda por SSID ou usuário;

4.51. Deverá suportar a autenticação com geração dinâmica de chaves criptográficas por sessão ou por usuário;

4.52. Possuir, em conjunto com o ponto de acesso Wi-Fi Protected Access (WPA2) com algoritmo de criptografia Advanced Encryption Standard (WPA2-AES), AES – 128 bits;

4.53. Possuir os seguintes controles/filtros nas camadas:

4.53.1. L2 – Baseado em MAC *Address* e *Client Isolation* por VLAN;

4.53.2. L3 – Baseado em endereço IP;

4.53.3. L4 – Baseado em portas TCP/UDP;

4.53.4. L7 – Baseado na Identificação de Aplicações.

4.54. Deverá conter mecanismos de Wireless Intrusion Protection (WIPS) para redes 802.11;

4.55. Deverá possuir mecanismo de autenticação entre cliente móvel e ponto de acesso para evitar ataques de camada 2 com foco em pacotes de gerenciamento como “association” e “disassociation”;

4.56. Deverá possuir todo software necessário para a implantação de qualquer funcionalidade exigida e qualquer outro recurso eventualmente necessário ao seu pleno funcionamento;

4.57. Tecnologia baseada em ***appliance*** **Físico:**

4.57.1. Deverá fornecer o todos os acessórios necessários para operacionalização do equipamento, tais como software, cabos lógicos, cabos de interface RS-232, cabos de energia elétrica e kit de fixação no rack padrão de 19';

4.57.2. Deverá ser montado em *rack* padrão de 19 (dezenove) polegadas, incluindo todos os acessórios necessários;

4.57.3. Possuir altura máxima de 1 (um) *rack unit* (1U);

4.57.4. Deverá possuir pelo menos, 2 (duas) portas 10 Gigabit Ethernet nos padrões 10GBASE-T, com possibilidade de negociação automática em 1GbE, sendo que a porta de console não será computada para atender essa exigência, caso seja entregue outro padrão de tecnologia na porta, deverá ser entregue o adaptador plenamente compatível com 10GBase-T sem prejuízo a este item.

4.57.5. Possuir fontes redundantes e alimentação interna com seleção automática de tensão (100-240V AC);

4.57.6. Possuir agregação de *links* seguindo o protocolo LACP;

5. Pacote de Licenças para usuários visitantes (500 usuários)

5.1. Fornecimento e garantia de pacotes de licenças para gerenciamento de dispositivos externos da rede wireless.

5.2. Cada pacote deve contemplar licenças para acesso de 500 (quinhentos) dispositivos simultâneos;

5.3. A solução deverá estar licenciada para os usuários visitantes, considerando apenas SSID visitantes;

5.4. A solução não deverá consumir do licenciamento os usuários conectados no SSID corporativo, apenas os usuários ativos no SSID visitantes;

5.5. Todas as licenças devem ser de caráter permanente e contínuo, de forma que a solução funcione mesmo após o término da garantia exigida;

5.6. Todas as licenças devem ser instaladas e configuradas sem qualquer ônus adicional.

6. Solução de Controle de Acesso

6.1. Permitir instalação em ambiente virtual *VMware ESXi* 6.0 ou superior;

6.2. Suporte aos sistemas operacionais RedHat Enterprise Linux ou CentOS 7 ou Windows Server 2012 ou superior, em plataforma de hardware padrão Intel;

6.3. Deverá permitir a criação de páginas personalizadas no portal web para o captive portal, com a inclusão de imagens, instruções em texto e campos de texto que possam ser preenchidos pelos clientes;

6.4. Deverá permitir o controle de acesso para todos os usuários vinculados às licenças do item 5, simultâneos, com capacidade de expansão futura para, no mínimo, 4.000 (quatro mil) usuários;

6.5. Deverá ser licenciado para, no mínimo, 2500 (dois mil e quinhentos) usuários internos simultâneos, autenticados no Active Directory ou via Radius, caso sejam necessárias as licenças para usuários internos, tais licenças não serão necessárias para a Solução de Controle de Acesso do Item 6, caso a Controladora Wireless do Item 4 possua nativamente a possibilidade de autenticar a quantidade informada de usuários internos via Active Directory ou Radius;

6.6. Deverá permitir nativamente ou em conjunto com a controladora o cadastramento de, no mínimo, 1.000 (mil) usuários visitantes;

6.7. Deverá possuir funcionalidade de busca por usuários já conhecidos (recorrentes), realizando a identificação do dispositivo móvel no ingresso e permissão de acesso do usuário sem a necessidade de nova autenticação;

6.8. Deve permitir a customização do formulário de criação de credenciais, a ser preenchido pelo visitante, em caso de “self-service”, especificando quais informações cadastrais dos visitantes são obrigatórias conforme o perfil, contendo, no mínimo, Nome, E-mail do usuário, CPF e Telefone;

6.9. Deverá permitir que o layout das telas de acesso sejam customizáveis com no mínimo 01 (um) logotipo e 01 (um) fundo de tela, com a utilização de texto e imagens em formatos JPEG ou PNG;

6.10. Deverá exigir que o usuário visitante aceite o “Termo de uso da rede” a cada login ou apenas no primeiro login;

6.11. Possuir capacidade de autenticação dos usuários visitantes através de senhas pré-cadastradas ou vouchers, para cada indivíduo ou grupo, no caso de eventos;

6.12. Deverá permitir que as contas de visitantes tenham validade controlada com período de validade da senha em quantidade de horas, dias e semanas;

6.13. Deverá possuir portal web seguro (SSL) a ser apresentado automaticamente aos usuários visitantes (temporários) durante a sua conexão com a rede;

6.14. Deverá possuir o envio das credenciais de acesso aos usuários registrados através de mensagens SMS (Short Message Service) ou email ou impressão local;

6.15. Deverá possuir múltiplos perfis de usuários administrativos com diferentes tipos de permissão;

6.16. Deverá possuir recurso de liberação de acesso por endereço MAC, onde o endereço do dispositivo pode ser cadastrado manualmente ou adicionado dinamicamente para os usuários que já realizaram acesso ao menos uma vez;

6.17. Deverá ter suporte ao provisionamento automático de dispositivos, através de Portal Captive para Windows, Mac OSX, iOS e Android.

6.18. O portal de autenticação deverá ser suportado, no mínimo, em um dos seguintes navegadores de Internet: Microsoft Edge ou Internet Explorer, Mozilla Firefox, e Chrome, operando em PCs e dispositivos móveis;

6.19. A solução deverá integrar com o Active Directory da Microsoft para identificação e autenticação dos usuários;

6.20. Deverá permitir o encaminhamento do tráfego de saída de usuários visitantes (guests) diretamente para a Internet, de forma totalmente separada do tráfego da rede corporativa;

6.21. Deverá permitir a configuração do número máximo de conexões simultâneas realizadas por uma mesma conta, possibilitando que um usuário possua mais de um dispositivo na rede com a mesma senha e que contas coletivas sejam utilizadas em eventos. Esta funcionalidade deve ser possível em usuários visitantes autenticados pelo captive portal;

6.22. Deverá possuir controle de acesso administrativo da solução baseado no perfil do usuário;

6.23. Deverá possuir protocolo de autenticação para controle do acesso administrativo da solução utilizando servidor Radius ou Microsoft Active Directory;

6.24. Deverá suportar IEEE 802.1x, com pelo menos os seguintes métodos EAP: EAP-TLS e PEAP-MSCHAPv2;

7. Serviços de instalação e configuração do Software de Gerência, Controladora Wireless, Licenças de Visitantes e Controle de Acesso (itens 1, 4, 5 e 6)

7.1. Os produtos referentes aos itens 1, 4, 5 e 6 deverão ser entregues, instalados e configurados nas dependências do Tribunal Regional Federal da 1ª Região, em Brasília-DF;

7.2. Todas as fases de planejamento da instalação e configuração deverão ser realizadas com a presença de técnicos da CONTRATADA, que deverão possuir capacidade técnica necessária à execução do serviço. Os serviços deverão ser executados por técnicos certificados pelo fabricante da solução;

7.3. A CONTRATADA deverá configurar todos os equipamentos, software e componentes necessários para o pleno funcionamento e operacionalidade da solução incluindo os seguintes escopos:

7.3.1. Configuração da autenticação dos usuários wireless por meio da base de usuários do servidor de diretório (AD) da CONTRATANTE, utilizando o protocolo IEEE 802.1x, de modo que o acesso do usuário seja liberado pela solução apenas após sua autenticação;

7.3.2. Configuração para permitir autenticação Web para estações de trabalho sem cliente 802.1x instalado;

7.3.3. Configuração para permitir autenticação pelo MAC Address, para dispositivos sem cliente 802.1x e sem browser;

7.3.4. Configuração de wIDS/wIPS;

7.3.5. Configuração para classificação/detecção de interferências WiFi e não-WiFi;

7.3.6. Configurar o controle de aplicações permitindo ao administrador filtrá-las para que seja obedecida a política de segurança adotada pela CONTRATANTE;

7.3.7. Criação de templates de configuração;

7.3.8. Criação de política de backup dos arquivos de configuração dos equipamentos;

7.3.9. Criação de política de acesso;

7.4. Deverá realizar a configuração de um portal de autenticação web (Capitive Portal) para os usuários servidores/visitantes, com as seguintes funcionalidades:

7.4.1. Funcionar de forma criptografada com o uso de certificados (SSL);

7.4.2. Criar um certificado auto-assinado;

7.4.3. Customizar com logotipo e políticas de acesso;

7.4.4. Check-box para aceite com as políticas de acesso da rede;

7.4.5. Configurar regras de acesso que permitem acessos a serviços específicos antes da autenticação, por exemplo, DHCP;

7.5. A configuração deverá ser executada de acordo com as recomendações do fabricante;

8. Serviços de instalação e configuração dos pontos de acesso e switches PoE (itens 2 e 3)

8.1. Os serviços de instalação e configuração especificados no item 02 serão realizados nos edifícios do TRF localizados no Distrito Federal, na respectiva localidade listada no Anexo II do Termo de Referência.

8.2. Uma unidade do Item 08 deste termo de referência é relativa à instalação de 01 (um) ponto de acesso e a instalação e configuração do Switch POE quando necessário;

8.3. O projeto de implantação, dos equipamentos, deve ser planejado e documentado previamente pela CONTRATADA em conjunto com o Contratante;

8.4. A instalação e configuração necessitam de aprovação prévia de Projeto de Implantação pelo Contratante para a quantidade CONTRATADA;

8.5. O Projeto de implantação deverá levar em consideração as peculiaridades, tais como, área a ser coberta pela rede e arquitetura do edifício (necessidade de manutenção em gesso, eletro calhas, cabos não aparentes e etc.) de cada área;

8.6. Ficarão a cargo da CONTRATADA o trabalho de fixação dos dispositivos, fornecimento e instalação dos dispositivos antifurto, conectorização de patch cords, configuração dos dispositivos e demais atividades técnicas necessárias para operacionalização dos pontos de acesso;

8.7. Ficarão a cargo da CONTRATADA a instalação, fixação e configurações dos switches PoE nos racks dos distribuidores;

8.8. CONTRATADA deverá providenciar os reparos em forros, divisórias, paredes e piso danificados em decorrência da atividade de instalação dos pontos de acesso, utilizando, para tal, material similar em qualidade e características técnicas;

8.9. Após a finalização das instalações dos pontos de acesso, a CONTRATADA deverá realizar a validação em campo por amostragem para medição de cobertura de sinal relação sinal/ruído, avaliação de canais, taxas de transmissão. Um equipamento especializado em análise de espectro e específico para este fim deve ser utilizado, não sendo aceitos notebooks e/ou smartphones com softwares que realizam o escaneamento de redes sem-fio;

8.10. A CONTRATADA deverá efetuar a passagem de cabos dentro do eletro calhas na estrutura existente das localidades listadas no Anexo II;

8.11. Deverá usar Copex metálico revestido de 1/2 polegada, onde não houver duto ou eletro calha para passagem do cabo de conexão do ponto de acesso (AP) fornecido pela CONTRATADA;

8.12. Deverá usar canaletas para acondicionar os cabos (não deverá existir cabo aparente);

8.13. Fixar os Patch Painel nos racks que se encontram na sala de telecomunicação nos andares preestabelecidos pelo Contratante;

8.14. Efetuar a instalação dos Patch cords interligando os Switches e os pontos de acesso (AP) nos andares;

8.15. Instalação e fornecimento de todo material passivo de rede (Patch cords, Patch painel, cabo UTP 4Px24AWG Categoria 6, conectores fêmea e macho RJ-45 Categoria 6);

8.16. Cabeamento para ligação de todos os pontos de acesso ao switch de infraestrutura mais próximo, distribuídos nas localidades citadas no Anexo II;

8.17. Certificação de todos os cabos utilizados na interligação dos pontos de acesso;

8.18. Identificação por meio de etiquetas do cabeamento realizado para instalação dos pontos de acesso;

8.19. O projeto prevê uma estimativa de 6.100 (Seis mil e cem) metros de cabos de Cat 6 a serem passados na eletro calhas distribuídas nas localidades listadas no Anexo II;

8.20. O projeto prevê uma estimativa 19 (dezenove) Pacht Painel Cat 6 de 24 portas a serem fixados em racks nas localidades listadas no Anexo II;

8.21. O projeto prevê uma estimativa de 300 (trezentos) mts de tubos Copex a serem fixados nas localidades listadas no Anexo II;

8.22. Os serviços deverão ser executados por técnicos certificados pelo fabricante da solução;

8.23. A configuração deverá ser executada de acordo com as recomendações do fabricante;

8.24. A CONTRATADA assumirá inteira responsabilidade por danos ou desvios eventualmente causados ao patrimônio do TRF ou de terceiros por ação ou omissão de seus empregados ou prepostos, quando da entrega, instalação e configuração da solução, na área de prestação dos serviços, mesmo que fora do exercício das atribuições previstas no contrato;

8.25. Os empregados da CONTRATADA envolvidos na implantação da solução, embora sujeitos a normas disciplinares ou convencionais do TRF, não terão com ele qualquer vínculo empregatício;

8.26. A CONTRATADA deverá incluir em seus custos todo o material e serviço necessário de cabeamento para a conexão dos controladores, pontos de acesso, passagem de cabos, fixação de tubos, fixação de Patch Painel e os demais elementos da solução rede sem fio (WLAN) das localidades citadas no Anexo II;

8.27. Será permitida a subcontratação de serviços como passagem do cabeamento, retirada, fixação de pontos de acesso, pinturas e reparos no forro de gesso. Está regra aplica-se exclusivamente ao ITEM 2 desta contratação;

8.28. Depois de concluída a instalação e configuração dos novos equipamentos a CONTRATADA deverá fornecer documentação (as built) da configuração final dos equipamentos, com endereçamentos IP's, localização física, interligação a outros equipamentos e demais informações necessárias à completa identificação da solução;

8.29. Todos os custos de deslocamentos, alimentação e hospedagem dos técnicos da CONTRATADA serão de inteira responsabilidade da CONTRATADA, não cabendo ao Contratante qualquer ônus adicional.

8.30. Só será considerada terminada a instalação quando a solução estiver em pleno funcionamento e os servidores devidamente treinados e habilitados para operação da mesma;

9. Treinamento

9.1. A Capacitação operacional habilitará a equipe técnica da CONTRATANTE a operar, configurar, gerenciar e manter a Solução de Rede Sem Fio;

9.2. O programa de capacitação operacional será tele presencial, em língua portuguesa, e deverá iniciar a qualquer tempo durante a Fase 1 – “Entrega dos Materiais” e deverá ser concluído até o final desta Fase 1;

9.3. A capacitação deverá ser realizada por profissionais certificados pelo fabricante dos equipamentos;

9.4. O programa de capacitação operacional deverá englobar todos os elementos constituintes da Solução de Rede Sem Fio contratada;

9.5. O programa de capacitação operacional deverá conter, no mínimo, o conteúdo programático de treinamentos oficiais do fabricante;

9.6. O(s) instrutor(es) deverá(ão) possuir certificação e habilitação emitidas pelo fabricante da solução ou por agentes expressamente autorizados a ministrar o programa, em todos os equipamentos e componentes utilizados na solução proposta;

9.7. Caberá à CONTRATADA prover todos os recursos didáticos necessários à realização do treinamento, incluindo, entre outros, equipamentos, licenças, notebook para apresentação, apostilas, blocos de anotações e canetas, entre outros;

9.8. Toda a documentação didática necessária aos cursos de treinamento deverá ser disponibilizada em papel impresso e mídia digital;

9.9. A CONTRATANTE poderá, a seu critério, reproduzir o material didático usado e treinar multiplicadores para repetir o treinamento sem custos adicionais, com vistas à retenção do conhecimento adquirido pela CONTRATANTE;

9.10. A capacitação operacional terá carga horária total de, pelo menos, 40 (sessenta) horas;

9.11. A capacitação operacional deverá incluir apostilas, manuais, exercícios práticos e laboratório para configuração de pontos de acesso e controlador WLAN;

9.12. O laboratório a ser utilizado deve possuir no mínimo 3 (três) pontos de acesso e 1 (um) software de gerencia/controladora WLAN iguais ou similares em funcionalidades aos produtos ofertados e devem ser fornecidos pela CONTRATADA;

9.13. Todos os módulos do programa de capacitação operacional serão ministrados para 10 (dez) participantes da equipe técnica da CONTRATANTE;

9.14. Os participantes serão divididos em duas turmas com 05 (cinco) integrantes cada;

9.15. A turma será exclusiva para a equipe da CONTRATANTE;

9.16. O programa será realizado em dias úteis em horário comercial;

9.17. A data de realização da Capacitação Operacional será definida entre a CONTRATANTE e a CONTRATADA;

9.18. Cada turma participará do programa em turnos distintos, cada um com no máximo 4 (quatro) horas de duração diária, em horários definidos pela CONTRATANTE;

9.19. O programa de capacitação operacional deverá contemplar, no mínimo, conteúdo do currículo oficial de cursos do fabricante, abrangendo, pelo menos, os seguintes módulos, realizados nos níveis intermediário ou avançado, a critério da equipe técnica da CONTRATANTE:

9.19.1. Padrões de rede sem fio 802.11 (802.11ac, 802.11n);

9.19.2. Arquiteturas de WLAN: Gerenciamento, Controladores e APs;

9.19.3. Visão geral da solução de rede sem fio contratada;

9.19.4. Visão geral dos equipamentos de rede sem fio adquiridos;

9.19.5. Administração e configuração do serviço de rede sem fio;

9.19.6. Operação da solução de gerência da rede sem fio;

9.19.7. Funcionalidades do serviço de rede sem fio;

9.19.8. Failover dos controladores;

9.19.9. Problemas mais frequentes e soluções adotadas (troubleshooting);

9.19.10. Outros tópicos relacionados com a solução de rede sem fio, em conformidade com o especificado neste edital.

9.20. A CONTRATADA deverá fornecer aos participantes do treinamento os certificados de conclusão de curso contendo, no mínimo:

9.20.1. Nome da instituição de ensino;

9.20.2. Nome do curso;

9.20.3. Nome do servidor capacitado;

9.20.4. Data de início e término da capacitação;

9.20.5. Carga horária;

9.20.6. Conteúdo programático;

9.20.7. Aproveitamento se for o caso.

9.21. Ao final do treinamento, os servidores participantes efetuarão uma avaliação do conteúdo ministrado. A qualidade será medida de 01 (um) a 10 (dez) pontos em cada um dos seguintes critérios:

9.21.1. Pontualidade;

9.21.2. Didática do instrutor;

9.21.3. Eficiência no repasse do conteúdo;

9.21.4. Adequação do treinamento ao conteúdo exigido no item 9.19 e subitens.

9.22. Caso a média das avaliações seja inferior a 7 (sete) pontos, a CONTRATADA deverá refazer o treinamento, após as adequações necessárias, especialmente de substituição do Instrutor, e sem qualquer custo adicional para o TRF 1ª Região, sendo que esse novo treinamento também será submetido aos mesmos critérios de avaliação;

10. Site Survey

10.1. Uma unidade deste Item é relativa a realização do site Survey para um edifício do TRF1, localizados no Distrito Federal, conforme item 17 do Termo de Referência

10.2. Deverá ser realizado o site survey preditivo, passivo e ativo no prédio, escopo desse projeto, descriminado na Ordem do Serviço;

10.3. O projeto deverá contemplar análise técnica (site survey) do ambiente físico, in loco, apoiada por software adequado, que indique:

10.3.1. Melhor posicionamento dos dispositivos de ponto de acesso para a maximização da cobertura do sinal de radiofrequência;

10.3.2. Informar a quantidade exata de pontos de acesso a serem instalados por andar no edifício;

10.3.3. Zonas de interferência;

10.3.4. A frequência a ser utilizada por cada ponto de acesso;

10.3.5. Mostrar as áreas de cobertura e as taxas de transmissão ou faixas de níveis de recepção de sinal de rádio frequência (RF) em desenho colorido;

10.3.6. Permitir a visualização de eventuais áreas sem cobertura de rádio frequência - RF (áreas de sombra), que foram realizadas pelo Site Survey;

10.3.7. Possibilitar, de forma nativa ou via software específico para este fim, gerar planta de cobertura prevista e planta de cobertura real (pós-ativação) com indicação gráfica da potência média para cada local da planta baixa;

10.3.8. Diagrama lógico da rede;

10.4. Os serviços deverão ser executados por técnicos certificados pelo fabricante da solução;

10.5. O Site Survey deverá ser executado de acordo com as recomendações do fabricante.